# Providing User Authentication Information to OAuth 2.0 Clients

Mike Jones

July 24, 2014

IETF 90

# draft-hunt-oauth-v2-user-a4c in a nutshell

- ID Token definition from OpenID Connect
  - Plus requiring “auth_time” claim always be present
- Several authorization request parameters from OpenID Connect, plus 2 new ones:
  - amr_values, ui_hint
- code_for_id_token response type
  - Requests ID Token be returned from Token Endpoint without returning an Access Token
- urn:ietf:params:oauth:grant-type:code-for-id-token grant type
  - Grant type used at token endpoint with codes from above
- Defines specific “amr” array element values:
  - pwd, pop, otp, fpt, eye, vbm, tel, sms, kba, wia, mfa

# Reasons It Exists and Relationships to OpenID Connect

- People were making up insecure authentication protocols using RFC 6749
  - Desire to define a simple authentication-only OAuth 2.0 profile so people would stop doing this
  - Note that using an authentication-only subset of OpenID Connect would also fill this need, if people would do so
- Desire for a code-style OAuth flow that returned identity claims but no Access Token
  - OpenID Connect enables this for the implicit flow but didn't define a way to do this for the code flow
- Desire to define specific authentication method reference ("amr") values
  - OpenID Connect explicitly decided not to do this

# Possible Factoring of Deliverables

- Specification defining OAuth code-style flow that returns an ID Token but no Access Token
  - Would define a response type and a grant type
- Specification defining “amr” claim values
  - And also “amr_values” request parameter
- Specification defining authentication request and response messages
  - Most of this could just reference OpenID Connect definitions, rather than duplicating them
  - New things could also be defined, e.g. “ui_hint”
- *These are mostly independent of one another*

# Questions to Working Group

- Which ones of the three possible deliverables do we want to pursue as a working group?
- Assuming the set is non-empty, should each of the three pursued be a separate draft, since they are largely independent?